

UNITED STATES DISTRICT COURT

for the

Western District of Washington

United States of America)

v.)

PAIGE A. THOMPSON) Case No. CR19-159RSL

Defendant)

SUBPOENA TO TESTIFY AT A HEARING OR TRIAL IN A CRIMINAL CASE

To: Amazon Web Services, Inc.
 Corporation Service Company
 300 Deschutes Way SW, Suite 208 MC-CSC1
 Tumwater, WA 98501

YOU ARE COMMANDED to appear in the United States district court at the time, date, and place shown below to testify in this criminal case. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place of Appearance: United States District Courthouse
 700 Stewart Street
 Seattle, WA 98101

Courtroom No.: Judge Lasnik, Ct. 15106

Date and Time: March 14, 2022 @ 10:00 a.m.

You must also bring with you the following documents, electronically stored information, or objects (*blank if not applicable*): SEE ATTACHMENT A

(SEAL)

Date: 11.24.21



CLERK OF COURT

Signature of Clerk or Deputy Clerk

Issued in Blank

The name, address, e-mail, and telephone number of the attorney representing (*name of party*) Paige Thompson
 _____, who requests this subpoena, are:

Nancy Tenney
 Assistant Federal Public Defender
 1601 5th Avenue, 7th Fl
 Seattle, WA 98101

Phone: (206) 553.1100
 Fax: (206) 553.0120

* please contact Investigator Stacey Brownstein at
 253.593.6710 if you have any questions. Please email the
 requested records to stacey_brownstein@fd.org

ATTACHMENT A

1. Any documents and communications relating to the Company's knowledge or awareness on or before March 12, 2019 of any misconfigurations of its cloud infrastructure, including any misconfigurations of the web application firewalls (or "WAFs") utilized by the Company and/or its customers, including Capital One Financial Corporation ("Capital One"), [REDACTED]

2. Any documents and communications involving anyone in the Company's Office of the Chief Information Security Officer relating to Paige Thompson's alleged exploitation of the Company's misconfigurations of its cloud infrastructure, including any misconfigurations of the WAFs utilized by the Company and/or its customers.

3. Any discovery-related correspondence, requests, and responses in Case No.: 19-cv-2947-AJT-JFA, in the Eastern District of Virginia. For example, this would include all of the Company's responses to requests for admissions or interrogatories, as well as letters discussing objections to discovery requests or productions of discovery.

4. Any unsolicited security advice related to reports of vulnerabilities of the Company's cloud infrastructure, including any misconfigurations of the WAFs utilized by the Company and/or its customers from March 12, 2019 through the present. For example, this would include reports from "white hats" or security researchers to the Company about any type of misconfigurations of its cloud infrastructure.

5. Any communications involving anyone in the Company's Office of the Chief Information Security Officer or any Executive Officers (e.g., CEO, CFO, GC, and CIO) of the Company with anyone at Capital One relating to (a) any misconfigurations of its cloud infrastructure, including any misconfigurations of the WAFs utilized by the Company and/or Capital One; and/or (b) Paige Thompson from March 12, 2019 until present.

6. Any documents and communications from April 1, 2019 through the present relating to a bug bounty program for the Company tied the Company's misconfiguration of its cloud infrastructure, including any misconfigurations of the WAFs utilized by the Company or its customers. For example, this would include its Vulnerability Research Program discussed on hackerone.com.

7. Any documents and communications from March 12, 2019 through present relating to the reasons why AWS developed and launched AWS EC2 instance metadata service ("IMDS") version 2, also known as IMDSv2.

8. Any contracts relating to cloud infrastructure and/or WAFs between the Company and one of the following parties: Capital One, [REDACTED]

9. Any bills and invoices for providing cloud infrastructure from January 1, 2019 through December 31, 2020 sent from the Company to the following entities: AWS, Capital One, [REDACTED]

DEFINITIONS:

1. The term “COMMUNICATION” is used in its broadest sense, and means any disclosure, transfer, exchange, or transmission of fact, information, advice, statement, or opinion by any means whatsoever, including, not limited to, oral, electronic, or written transmissions.
2. The term “DOCUMENT” is used in its broadest sense, and is defined to be synonymous in meaning and equal in scope to the definition in Federal Rule of Civil Procedure 34. A draft or non-identical copy is a separate DOCUMENT within the meaning of this term. Without limiting the generality of the foregoing, the term “DOCUMENT” means, without limitation, the following items, whether printed, or written, produced or reproduced by any other mechanical process, or written or produced by hand, or in electronic format: agreements, communications, reports, correspondence, telegrams, memoranda, summaries or records of telephone conversations, summaries or records of personal conversations or interviews, diaries, graphs, reports, notebooks, plans, drawings, sketches, maps, summaries or records of any meetings or conferences, summaries or reports of investigations or negotiations, opinions or reports of consultants, photographs, screenshots, motion picture film, tape recordings, videotapes, computer disks, tapes or hard drives, electronic mail, brochures, pamphlets, advertisements, circulars, newspaper or magazine articles, newsletters, publications, press releases, surveys, judicial records, customer lists, governmental certificates, applications, licenses, registrations, letters, accounts, objects, minutes of meetings, interoffice communications, studies, written forecasts, projections, analyses, contracts, guarantee agreements, ledgers, books of accounts, vouchers, checks, purchase orders, invoices, charge slips, expense account reports, receipts, working papers, drafts, statistical records, cost sheets, calendars, appointment books, time sheets or logs, job or transaction files, computer printouts or papers similar to any of the foregoing, and any marginal comments appearing on any DOCUMENT and other writing.
3. The term “INCLUDING” means including, but not limited to, the referenced items or subject matter.
4. The term “RELATING TO” means reflecting, regarding, concerning, identifying, describing, discussing, summarizing, evidencing, referencing, or commenting on the subject matter of the Subpoena Request.
5. The term “COMPANY” means and refers to Amazon Web Services, Inc. and any of its employees, officers, directors, successors, predecessors, affiliates, divisions, parents, subsidiaries, vendors, contractors, representatives, agents and anyone acting on or for its behalf.
6. The term “ANY” includes the term “all,” and vice versa; the singular form of a noun or pronoun shall include the plural form of the noun or pronoun, and vice versa; the neutral form of a pronoun shall include the masculine and feminine forms of the pronoun, and vice versa; and the use of any tense of any verb shall include all other tenses of the verb. In each such instance, the Subpoena Request shall be construed so as to furnish the most complete and inclusive answer.

Case No. CR18-5489BHS

PROOF OF SERVICE

This subpoena for *(name of individual and title, if any)* _____
 was received by me on *(date)* _____.

☐ I served the subpoena by delivering a copy to the named person as follows: _____

_____ on *(date)* _____; or

☐ I returned the subpoena unexecuted because: _____

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also
 tendered to the witness fees for one day's attendance, and the mileage allowed by law, in the amount of

\$ _____.

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ 0.00.

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc: